UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/943,709	08/31/2001	Brig Barnum Elliott	BBNT-P01-139	2582

28120   7590   03/31/2005

FISH & NEAVE IP GROUP
ROPES & GRAY LLP
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER
SHERKAT, AREZOO

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/943,709	ELLIOTT, BRIG BARNUM
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _31 August 2001_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-53_ is/are pending in the application.

   4a) Of the above claim(s) _27-32 and 45-53_ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-26 and 33-44_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) _1-53_ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _31 August 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)   4)☐ Interview Summary (PTO-413)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)   Paper No(s)/Mail Date. _____ .
3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)   5)☐ Notice of Informal Patent Application (PTO-152)
   Paper No(s)/Mail Date _8/31/2001_.   6)☐ Other: _____ .

DETAILED ACTION

Claims 1-53 are presented for examination.

Election/Restrictions

Restriction to one of the following inventions is required under 35 U.S.C. 121:

I.   Claims 1-26 and 33-44, drawn to Key distribution in a multi-node

communication network using cryptography, classified in class 380,

subclass 278.

II.   Claims 27-32 and 45-53, drawn to Key distribution in an optical network

using cryptography, classified in class 380, subclass 256.

The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as combination and subcombination. Inventions in

this relationship are distinct if it can be shown that (1) the combination as claimed does

not require the particulars of the subcombination as claimed for patentability, and (2)

that the subcombination has utility by itself or in other combinations (MPEP §

806.05(c)). In the instant case, the combination as claimed does not require the

particulars of the subcombination as claimed because a network may or may not be an

optical network. The subcombination has separate utility such as fiber optics networks.

Because these inventions are distinct for the reasons given above and the

search required for Group II is not required for Group I, restriction for examination

purposes as indicated is proper.

During a telephone conversation with Mr. Edward Gordon on 03/25/2005, claims

27-32 and 45-53 are withdrawn from further consideration by the examiner, 37

CFR 1.142(b), as being drawn to a non-elected invention.

Claims 1-26 and 33-44 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the
> United States before the invention thereof by the applicant for patent, or on an international application
> by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this
> title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act

of 1999 (AIPA) and the Intellectual Property and High Technology Technical

Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting

directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior

to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1, 9-15, 33, and 43-44 are rejected under 35 U.S.C. 102(e) as being

anticipated by Mayers et al., (U.S. Patent No. 6,678,379 and Mayers hereinafter).

Regarding claims 1 and 13-14, Mayers discloses a method of establishing a path for distributing data through a network, comprising:

establishing a first data distribution path through the network, the network comprising at least one switch and one link, determining whether eavesdropping has occurred on the first data distribution path using quantum cryptography, and establishing a second data distribution path through the network based on the eavesdropping determination (Col. 3, lines 12-67).

Regarding claim 15, Mayers discloses a system for establishing a path for distributing data through a network, comprising:

a switch configured to establish a first encryption key distribution path through the network, the first encryption key distribution path comprising a plurality of switches and links (i.e., sender works as a switch to establish another quantum channel to send the shared key), and a data distribution endpoint configured to determine whether eavesdropping has occurred on the first encryption key distribution path using quantum cryptography, wherein the switch is further configured to establish a second encryption key distribution path through the network responsive to the eavesdropping determination, the second encryption key distribution path comprising a plurality of switches and links (Col. 3, lines 12-67).

Regarding claims 33 and 44, Mayers discloses a method of routing around eavesdroppers in a network, comprising:

establishing a first path in the network, transmitting data symbols over the first

path, identifying eavesdropping on the first path using quantum cryptography,

establishing a second path in the network responsive to the eavesdropping

identification, and transmitting data symbols over the second path (Col. 8, lines 46-67

and Col. 9, lines 1-49).

Regarding claim 43, Mayers discloses quantum encryption key distribution

device, comprising:

a transceiver, and a processing unit configured to: establish a first key

distribution path in the network, the first key distribution path comprising a plurality of

links and switches, transmit at least a portion of a first encryption key over the first key

distribution path via the transceiver, identify eavesdropping on the first key distribution

path using quantum cryptographic techniques, establish a second key distribution path

in the network responsive to the eavesdropping identification, the second key

distribution path comprising a plurality of links and switches, and transmit at least a

portion of a second encryption key over the second key distribution path via the

transceiver (Col. 8, lines 46-67 and Col. 9, lines 1-49).

Regarding claims 9 and 11, Mayer discloses further comprising: distributing a

first encryption key via the first encryption key distribution path (Col. 3, lines 28-50).

Regarding claims 10 and 12, Mayer discloses further comprising: distributing a

second encryption key via the second encryption key distribution path (i.e., in the event

of eavesdropping the session is restarted from the scratch, which means that another

set of random number series are used, and the measures are taken to check the

quantum channel, or switching to another quantum channel)(Col. 3, lines 28-50).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-8, 16-26, and 34-42 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Mayers et al., (U.S. Patent No. 6,678,379 and Mayers hereinafter), in

view of Doverspike, (U.S. Patent No. 6,097,696 and Doverspike hereinafter).

Teachings of Mayers regarding limitations of claim 1 have been discussed

previously.

Regarding claims 16 and 24-26, Mayers discloses a method for testing the

security of a quantum cryptographic system used for quantum key distribution and in the

event of eavesdropping restarting the session form the beginning or switching to
another channel (Col. 1, lines 1-64).

Mayers does not expressly disclose requesting a path through the network, the
request comprising identifiers of at least one of a link and a node in the network, and
setting up the path through the network, the path excluding the at least one of the link
and the node in the network.

However, Doverspike discloses sending and/or receiving a request for a path
through the network, the request comprising identifiers of at least one of a link and a
node in the network (i.e., the messages are routed in accordance with the information in
table 2, by including the full node path in each message)(Col. 9, lines 5-29), and setting
up the path through the network, the path excluding the at least one of the link and the
node in the network (Col. 8, lines 44-67 and Col. 9, lines 1-45).

Therefore, it would have been obvious to a person of ordinary skill in the art at
the time of applicant's invention to modify the key distribution method of Mayers by
including setting up the path through the network, the path excluding the at least one of
the link and the node in the network as disclosed by Dovespike. This modification
would have been obvious because one of ordinary skill in the art would have been
motivated by the suggestion of Doverspike to provide for a reroute path that avoids the
failed condition (i.e., eavesdropping) and restores communication within the network
(Doverspike, Col. 2, lines 7-16).

Regarding claims 2, 23, and 34, Mayers discloses wherein the communication network is an optical network (Col. 1, lines 64-67 and Col. 2, lines 1-52)

Regarding claims 3, 20, and 35, Mayers does not expressly disclose wherein the multi-node communications network comprises optical switches.

However, Doverspike discloses wherein the multi-node communications network comprises optical switches (i.e., switch fabric 12 in each subnetwork)(Col. 2, lines 35-67 and Col. 3, lines 1-45).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the key distribution method of Mayers by including a multi-node communications network comprises optical switches as disclosed by Dovespike. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doverspike to provide for a reroute path that avoids the failed condition (i.e., eavesdropping) and restores communication within the network (Doverspike, Col. 2, lines 7-16).

Regarding claims 4, 21, and 36, Mayers does not expressly disclose wherein the optical switches are interconnected via links.

However, Doverspike discloses wherein the optical switches are interconnected via links (Col. 3, lines 45-67 and Col. 4, lines 1-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the key distribution method of Mayers by

including wherein optical switches are interconnected via links as disclosed by
Dovespike. This modification would have been obvious because one of ordinary skill in
the art would have been motivated by the suggestion of Doverspike to provide for a
reroute path that avoids the failed condition (i.e., eavesdropping) and restores
communication within the network (Doverspike, Col. 2, lines 7-16).

Regarding claims 5-6 and 37-38, Mayers does not expressly disclose wherein
the first and the second path comprises a plurality of links and switches.

However, Doverspike discloses wherein the first and the second path comprises
a plurality of links and switches (Col. 3, lines 45-67 and Col. 4, lines 1-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at
the time of applicant's invention to modify the key distribution method of Mayers by
including wherein the first and the second path comprises a plurality of links and
switches as disclosed by Dovespike. This modification would have been obvious
because one of ordinary skill in the art would have been motivated by the suggestion of
Doverspike to provide for a reroute path that avoids the failed condition (i.e.,
eavesdropping) and restores communication within the network (Doverspike, Col. 2,
lines 7-16).

Regarding claims 7 and 39, Mayers does not expressly disclose wherein the first
path and the second path comprise no common links and switches.

However, Doverspike discloses wherein the first path and the second path comprise no common links and switches (Col. 9, lines 30-45).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the key distribution method of Mayers by including wherein the first path and the second path comprise no common links and switches as disclosed by Dovespike. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doverspike to ensure that the message is transmitted over the surviving links (Doverspike, Col. 9, lines 40-45).

Regarding claims 8 and 40, Mayers does not expressly disclose wherein the first path and the second path comprise of a subset of common links and switches.

However, Doverspike discloses wherein the first path and the second path comprise of a subset of common links and switches (Col. 5, lines 3-67 and Col. 6, lines 1-65).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the key distribution method of Mayers by including wherein the first path and the second path comprise of a subset of common links and switches as disclosed by Dovespike. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doverspike to provide for a minimum number of nodes required to maintain connectivity (Doverspike, Col. 6, lines 1-6).

Regarding claim 17, Mayers does not expressly disclose wherein setting up the

path through the network comprises: constructing a first graph of a topology of the

network.

However, Doverspike discloses wherein setting up the path through the network

comprises: constructing a first graph of a topology of the network (i.e., topology is the

configuration of the communication network, therefore, any multi-node network

communication follows some sort of a topological routing method such as ring, mesh,

star, and etc.)(Col. 1, lines 18-53 and Col. 4, lines 20-67 and Col. 5, lines 1-2).

Therefore, it would have been obvious to a person of ordinary skill in the art at

the time of applicant's invention to modify the key distribution method of Mayers by

including constructing a first graph of a topology of the network as disclosed by

Dovespike. This modification would have been obvious because one of ordinary skill in

the art would have been motivated by the suggestion of Doverspike to provide for a

reroute path that avoids the failed condition (i.e., eavesdropping) and restores

communication within the network (Doverspike, Col. 2, lines 7-16).

Regarding claim 18, Mayers does not expressly disclose wherein setting up the

path through the network further comprises: constructing a second graph of a topology

of the network by omitting the at least one of a link and node in the network from the

first graph.

However, Doverspike discloses wherein setting up the path through the network further comprises: constructing a second graph of a topology of the network by omitting the at least one of a link and node in the network from the first graph (Col. 1, lines 17-67 and Col. 2, lines 1-16).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the key distribution method of Mayers by including constructing a second graph of a topology of the network by omitting the at least one of a link and node in the network from the first graph as disclosed by Dovespike. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doverspike to provide for a reroute path that avoids the failed condition (i.e., eavesdropping) and restores communication within the network (Doverspike, Col. 2, lines 7-16).

Regarding claim 19, Mayers does not expressly disclose wherein setting up the path through the network further comprises: determining a shortest path through the second graph.

However, Doverspike discloses wherein setting up the path through the network further comprises: determining a shortest path through the second graph (Col. 9, lines 5-45).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the key distribution method of Mayers by including determining a shortest path through the second graph as disclosed by

Dovespike. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doverspike to provide for an efficient reroute path that avoids the failed condition (i.e., eavesdropping) and restores communication within the network (Doverspike, Col. 2, lines 7-16).

Regarding claim 22, Mayers discloses wherein the links comprise one or more optical fibers (Col. 1, lines 64-67 and Col. 2, lines 1-21).

Regarding claim 41, Mayers discloses wherein the data symbols comprise at least a portion of an encryption key (Col. 3, lines 28-59).

Regarding claim 42, Mayers discloses wherein the data symbols comprise polarized photons (Col. 1, lines 64-67 and Col. 2, lines 1-21).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Townsend, (U.S. Patent No. 5,675,648),

Medard et al., (U.S. Patent No. 6,507,012), and

Townsend, (U.S. Patent No. 5,768,378).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Arezoo Sherkat
Patent Examiner
Group 2131
March 30, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100